(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10241287 A**

(43) Date of publication of application: **11.09.98**

(51) Int. Cl **G11B 20/10**

(21) Application number: **09040529**

(22) Date of filing: **25.02.97**

(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

(72) Inventor: **KUNIHIRA TADASHI**

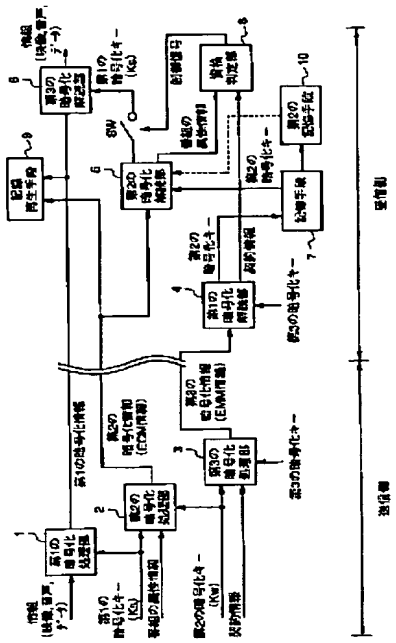
# (54) DIGITAL INFORMATION RECORDING/REPRODUCING DEVICE

(57) Abstract:

PROBLEM TO BE SOLVED: To reproduce recorded digital information for a specified period without reducing security by using a digital information ciphering transmission system constructed for deciphering second ciphering information reproduced by a recording/reproducing means by using a second ciphering key held in a first or second storage means.

SOLUTION: The storage means 7 of a digital information recording/ reproducing device receives and holds a second ciphering key outputted from a first cryptoanalysis section 4 and then outputs this to a second cryptoanalysis section 5. The held second ciphering key is also outputted to a second storage means 10 and held there for a fixed period. When a recording/reproducing means 9 reproduces the recorded first or second ciphering information, the second cryptoanalysis section 5 for decoding the second ciphering information decodes the reproduced second ciphering information by using the second ciphering key held in the first or second storage means 7 or 10.





(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－241287

(43)公開日　平成10年(1998)９月11日

| (51)Int.Cl.[6] | 識別記号 | ＦＩ | |
|---|---|---|---|
| Ｇ１１Ｂ　20/10 | | Ｇ１１Ｂ　20/10 | Ｈ |

審査請求　未請求　請求項の数８　ＯＬ　（全 19 頁）

(21)出願番号　特願平9－40529

(22)出願日　平成９年(1997)２月25日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　國平　宰司
大阪府門真市大字門真1006番地　松下電器産業株式会社内

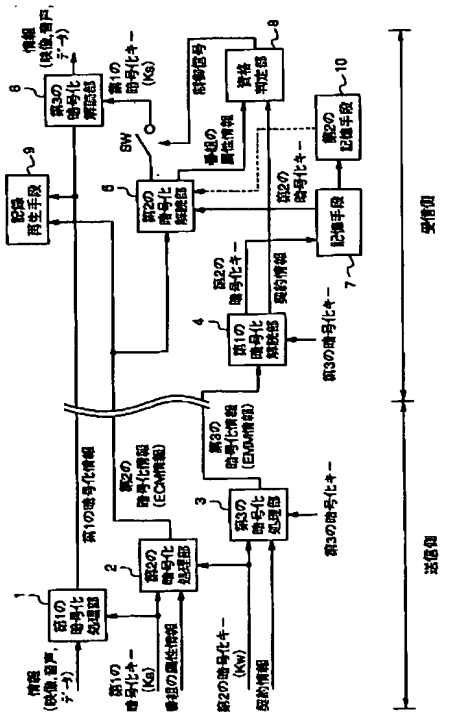
(74)代理人　弁理士　早瀬　憲一

(54)【発明の名称】　ディジタル情報記録再生装置

(57)【要約】

【課題】　システムにおけるセキュリティを低下させることなく、所定の期間は、記録したディジタル情報の再生を可能とできるディジタル情報記録再生装置を得る。

【解決手段】　記憶手段７に保持している第２の暗号化キーを記憶手段７のデータ変更後一定期間保持する第２の記憶手段１０を備え、第１，第２の暗号化情報を記録，再生する記録再生手段９が、記録した第１，第２の暗号化情報を再生するときに、第２の暗号化情報（ＥＣＭ情報）を解読する第２の暗号化解読部が、前記記録再生手段が再生した第２の暗号化情報を、前記第１または第２の記憶手段に保持された第２の暗号化キーを用いて暗号を解除する構成とした。



1

【特許請求の範囲】

【請求項１】　放送局より伝送される、情報を第１の期間ごとに変化する第１の暗号化キーを用いて暗号化した第１の暗号化情報，前記第１の暗号化キーと前記情報の属性情報を第２の期間ごとに変化する第２の暗号化キーにより暗号化した第２の暗号化情報，及び次の第２の期間に有効な第２の暗号化キーと個別の契約情報を第３の暗号化キーにより暗号化した第３の暗号化情報を受信する手段と、

受信した第３の暗号化情報を前記第３の暗号化キーを用いて暗号を解除して前記第２の暗号化キーと前記個別の契約情報を出力する第１の暗号化解読部と、

該第１の暗号化解読部が出力する第２の暗号化キーを次の第２の期間の間保持する第１の記憶手段と、

受信した第２の暗号化情報を、一つ前の第２の期間に得られ前記第１の記憶手段に保持された第２の暗号化キーを用いて暗号を解除して前記第１の暗号化キーと前記情報の属性情報を出力する第２の暗号化解読部と、

受信した第１の暗号化情報を、前記第２の暗号化解読部より出力され、前記第１の暗号化解読部より出力された個別の契約情報と前記第２の暗号化解読部より出力された情報の属性情報との比較に基づいて与えられる、第１の暗号化キーを用いて暗号を解除して前記情報を得る第３の暗号化解読部と、

受信した第１，及び第２の暗号化情報を記録，再生する記録再生手段と、

前記第１の記憶手段に保持している第２の暗号化キーを前記第１の記憶手段のデータ変更後一定期間保持する第２の記憶手段とを備え、

前記記録再生手段に記録された情報の再生時に、前記第２の暗号化解読部が、前記記録再生手段が再生した第２の暗号化情報を、前記第１または第２の記憶手段に保持された第２の暗号化キーを用いて暗号を解除することを特徴とするディジタル情報記録再生装置。

【請求項２】　請求項１記載のディジタル情報記録再生装置において、

前記記録再生手段は、第１，第２の暗号化情報とともに記録時の時間情報を記録することを特徴とするディジタル情報記録再生装置。

【請求項３】　請求項２記載のディジタル情報記録再生装置において、

前記記録再生手段に記録された第１，第２の暗号化情報を、該第１，第２の暗号化情報が前記記録再生手段に記録された時から上記第２の記憶手段が第２の暗号化キーを保持する上記一定期間を上限とする所定期間に限り再生可能とする制御手段をさらに備えたことを特徴とするディジタル情報記録再生装置。

【請求項４】　請求項１または請求項３記載のディジタル情報記録再生装置において、

前記記録再生手段は、第１，第２の暗号化情報とともに、記録される第２の暗号化情報の解読に有効な第２の暗号化キーが何であるかを示す暗号化キー識別情報を記録することを特徴とするディジタル情報記録再生装置。

【請求項５】　請求項１ないし請求項４のいずれかに記載のディジタル情報記録再生装置において、

前記第１の暗号化解読部，第２の暗号化解読部，第１の記憶手段，及び第２の記憶手段が、ディジタル情報記録再生装置本体に対し着脱自在の電子回路ユニットに搭載されていることを特徴とするディジタル情報記録再生装置。

【請求項６】　放送局より伝送される、情報を第１の期間ごとに変化する第１の暗号化キーを用いて暗号化した第１の暗号化情報，前記第１の暗号化キーと前記情報の属性情報を第２の期間ごとに変化する第２の暗号化キーにより暗号化した第２の暗号化情報，及び次の第２の期間に有効な第２の暗号化キーと個別の契約情報を第３の暗号化キーにより暗号化した第３の暗号化情報を受信する手段と、

受信した第３の暗号化情報を前記第３の暗号化キーを用いて暗号を解除して前記第２の暗号化キーと前記個別の契約情報を出力する第１の暗号化解読部と、

該第１の暗号化解読部が出力する第２の暗号化キーを次の第２の期間の間保持する記憶手段と、

受信した第２の暗号化情報を、一つ前の第２の期間に得られ前記第１の記憶手段に保持された第２の暗号化キーを用いて暗号を解除して前記第１の暗号化キーと前記情報の属性情報を出力する第２の暗号化解読部と、

受信した第１の暗号化情報を、前記第２の暗号化解読部より出力され、前記第１の暗号化解読部より出力された個別の契約情報と前記第２の暗号化解読部より出力された情報の属性情報との比較に基づいて与えられる、第１の暗号化キーを用いて暗号を解除して前記情報を得る第３の暗号化解読部と、

受信した第３の暗号化情報を次の第２の期間の間保持する暗号化情報保持手段と、

受信した第１，及び第２の暗号化情報と前記暗号化情報保持手段に保持された一つ前の第２の期間に受信した第３の暗号化情報を記録，再生する記録再生手段とを備えたことを特徴とするディジタル情報記録再生装置。

【請求項７】　請求項６記載のディジタル情報記録再生装置において、

上記第３の暗号化解読部は、再生時の直前に取得した個別の契約情報と前記第２の暗号化解読部より出力された情報の属性情報との比較に基づいて与えられる、第１の暗号化キーを用いて、上記記録再生手段が再生する第１の暗号化情報の暗号を解除するものであることを特徴とするディジタル情報記録再生装置。

【請求項８】　請求項６記載のディジタル情報記録再生装置において、

記録時の個別の契約情報を保持する契約情報保持手段を

さらに備え、

上記第３の暗号化解読部は、上記契約情報保持手段が保持する記録時の個別の契約情報と前記第２の暗号化解読部より出力された情報の属性情報との比較に基づいて与えられる、第１の暗号化キーを用いて、上記記録再生手段が再生する第１の暗号化情報の暗号を解除するものであることを特徴とするディジタル情報記録再生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、放送局から暗号化されて伝送されるディジタル情報を記録再生するディジタル情報記録再生装置に関するものである。

【０００２】

【従来の技術】図７は、ディジタル情報を暗号化して伝送する際の放送局側における暗号化処理のための構成（放送側）及び従来のディジタル情報記録再生装置（受信側）の構成を示す図であり、図において、１は映像情報，音声情報，及びデータを含むディジタル番組情報を第１の暗号化キー（Ｋｓ）を用いて暗号化して第１の暗号化情報を出力する第１の暗号化処理部、２は第１の暗号化キー（Ｋｓ）と上記番組情報の番組の属性情報を第２の暗号化キー（Ｋｗ）を用いて暗号化して第２の暗号化情報（ＥＣＭ情報）を出力する第２の暗号化処理部、３は第２の暗号化キー（Ｋｗ）と受信者の個別の契約情報を第３の暗号化キーを用いて暗号化して第３の暗号化情報（ＥＭＭ情報）を出力する第３の暗号化処理部である。

【０００３】ここで、第１の暗号化キー（Ｋｓ）は第１の期間（数秒）ごとに異なる暗号化キーに切り替わるものであり、第２の暗号化キー（Ｋｗ）は第２の期間（１ヶ月～１年）ごとに異なる暗号化キーに切り替わるものである。また、第３の暗号化キーは受信の契約等をした時点で契約者に対して与えられるものであり、通常は切り替わることのないものである。

【０００４】また、４は受信した第３の暗号化情報（ＥＭＭ情報）をあらかじめ与えられた第３の暗号化キーを用いて解読し、第２の暗号化キーと契約情報を得る第１の暗号化解読部、７は第１の暗号化解読部４が出力する第２の暗号化キーを記憶し、一つ前の第２の期間に記憶した第２の暗号化キーを出力する記憶手段である。５は受信した第２の暗号化情報（ＥＣＭ情報）を記憶手段７が出力する一つ前の第２の期間に受信した第２の暗号化キーを用いて解読し、第１の暗号化キーと番組の属性情報を得る第２の暗号化解読部、６は受信した第１の暗号化情報を第１の暗号化キーを用いて解読し、情報（映像，音声，データ）を得る第３の暗号化解読部である。８は第２の暗号化解読部５で得られた番組の属性情報と第１の暗号化解読部４で得られた契約情報とを比較して契約者が当該番組を視聴する資格を有するか否かの判定を行なう資格判定部であり、資格の有無に応じた制御信号を出力し、第１の暗号化キー（Ｋｓ）を第３の暗号化解読部６に与えるか否かのスイッチングを行なう。



【０００５】図８は記憶手段７の構成を示す図である。図に示すように、記憶手段７は、第１の暗号化解読部４が出力する第２の暗号化キーを受け取ってこれを保持する第１の記憶領域７ａと、一つ前の第２の期間に受け取った第２の暗号化キーを保持しこれを第２の暗号化解読部５に対し出力する第２の記憶領域７ｂとを備えている。第１の記憶領域７ａに保持された第２の暗号化キーは第２の期間が切り替わったとき、すなわち、第１の暗号化解読部４から受け取る第２の暗号化キーが変化するタイミングで第２の記憶領域７ｂに移され、それ以前に第２の記憶領域７ｂに保持されていた第２の暗号化キーは消去される。第１の記憶領域７ａと第２の記憶領域７ｂとの間でこのような保持情報の受け渡しの動作が行なわれることにより、記憶手段７からは、常に、一つ前の第２の期間に取得した第２の暗号化キーが第２の暗号化解読部５に対して出力されるものである。

【０００６】映像情報，音声情報，及びデータを含むディジタル番組情報は第１の暗号化処理部１において第１の暗号化キー（Ｋｓ）を用いて暗号化され、第１の暗号化情報として伝送される。第１の暗号化キー（Ｋｓ）は第１の期間（数秒）ごとに異なる暗号化キーに切り替わるものであり、受信側で第１の暗号化情報の解読を可能とするために、この順次切り替わる第１の暗号化キー（Ｋｓ）は番組の属性情報とともに第２の暗号化処理部２において第２の暗号化キー（Ｋｗ）を用いて暗号化され、第２の暗号化情報（ＥＣＭ情報）として伝送される。第２の暗号化キー（Ｋｗ）は受信者の個別の契約情報とともに第３の暗号化処理部３において第３の暗号化キーを用いて暗号化され、第３の暗号化情報（ＥＭＭ情報）として伝送される。第２の暗号化キー（Ｋｗ）は第２の期間（１ヶ月～１年）ごとに異なる暗号化キーに切り替わるものであり、ある第２の期間に伝送される第２の暗号化情報（ＥＣＭ情報）を解読するための第２の暗号化キーは、その第２の期間の一つ前の第２の期間に第３の暗号化情報に含まれて伝送される。

【０００７】ディジタル情報記録再生装置側（受信側）では、第１の暗号化解読部４が、あらかじめ与えられている第３の暗号化キーを用いて第３の暗号化情報（ＥＭＭ情報）の暗号化を解読し、第２の暗号化キー，及び個別契約情報を得る。取得された第２の暗号化キーは記憶手段７の第１の記憶領域７ａに保持され、個別契約情報は資格判定部８に入力される。一方、第２の暗号化解読部５は、記憶手段７の第２の記憶領域７ｂに保持された一つ前の第２の期間に受信した第２の暗号化キーを用いて第２の暗号化情報（ＥＣＭ情報）を解読し、第１の暗号化キー（Ｋｓ），及び番組の属性情報を得る。資格判定部８は、第１の暗号化解読部４から得た個別の契約情報と第２の暗号化解読部５から得た番組の属性情報とを

比較して、契約者が当該番組を視聴する資格を有するか否かの判定をし、判定結果に応じた制御信号を出力する。スイッチＳＷは資格判定部８からの制御信号に応じて、第２の暗号化解読部で得られた第１の暗号化キー（Ｋｓ）を第３の暗号化解読部６に対して提供，非提供のスイッチングを行なう。また、第３の暗号化解読部６は、第２の暗号化解読部で得られスイッチＳＷを介して提供される第１の暗号化キー（Ｋｓ）を用いて第１の暗号化情報を解読し、番組の情報（映像，音声，データ）を得る。

【０００８】図９は、第２の期間と第１暗号化キー（Ｋｓ），第２の暗号化キー（Ｋｗ）との関係を示すタイミングチャート図である。図において、上述もしたように、放送局側から第２の暗号化情報（ＥＣＭ情報）に含まれて送信される第１の暗号化キーは、第２の期間の切り替わりとは無関係に第１の期間（数秒）毎に切り替わる。一方、第３の暗号化情報（ＥＭＭ情報）に含まれて放送局側から送信される第２の暗号化キー，及び第２の暗号化情報（ＥＣＭ情報）の解読に有効な第２の暗号化キーは第２の期間毎に切り替わる。図９において、Ｔ１の期間に第２の暗号化情報（ＥＣＭ情報）の解読に有効な第２の暗号化キーはＫｗ１であり、Ｔ２の期間に第２の暗号化情報（ＥＣＭ情報）の解読に有効な第２の暗号化キーはＫｗ２であり、Ｔ３の期間に第２の暗号化情報（ＥＣＭ情報）の解読に有効な第２の暗号化キーはＫｗ３である。また、Ｔ１の期間に放送局側から送信される第３の暗号化情報（ＥＭＭ情報）に含まれて放送局側から送信される第２の暗号化キーはＫｗ２であり、Ｔ２の期間に放送局側から送信される第３の暗号化情報（ＥＭＭ情報）に含まれて放送局側から送信される第２の暗号化キーはＫｗ３であり、Ｔ３の期間に放送局側から送信される第３の暗号化情報（ＥＭＭ情報）に含まれて放送局側から送信される第２の暗号化キーはＫｗ４である。このように、ある第２の期間に放送局側から送信される第２の暗号化情報（ＥＣＭ情報）の解読に有効な第２の暗号化キーは、一つ前の第２の期間に放送局側から送信される第３の暗号化情報（ＥＭＭ情報）に含まれて放送局側から送信される第２の暗号化キーである。

【０００９】次に、従来のディジタル情報記録再生装置におけるディジタル情報の記録再生動作について説明する。

【００１０】図示しない制御手段より情報記録の指示を受けて、記録再生手段９は、第１の暗号化情報，及び第２の暗号化情報（ＥＣＭ情報）を記録媒体に記録する。再生時には、再生した第２の暗号化情報（ＥＣＭ情報）を第２の暗号化解読部５に対して出力し、再生した第１の暗号化情報を第３の暗号化解読部６に対して出力する。この再生時に記憶手段７からは、この再生時が属する第２の期間の一つ前の第２の期間に第３の暗号化情報（ＥＭＭ情報）に含まれて放送局側から送信された第２



の暗号化キーが出力される。例えば、図９において、Ｔ２の期間に再生を行なう場合は、記憶手段７から出力される第２の暗号化キーはＫｗ２であり、Ｔ３の期間に再生を行なう場合は、記憶手段７から出力される第２の暗号化キーはＫｗ３である。一方、図９において、Ｔ２の期間に記録された第２の暗号化信号（ＥＣＭ情報）の解読に有効な第２の暗号化キーはＫｗ２であるので、このＴ２の期間に記録された第２の暗号化信号（ＥＣＭ情報）は、Ｔ２の期間に再生を行なう場合にのみその解読が可能であり、Ｔ３以降の期間に再生を行なった場合にはその解読を行なうことはできない。すなわち、Ｔ２の期間に記録されたディジタル情報は、Ｔ２の期間にのみその再生を行なうことができるものである。

【００１１】

【発明が解決しようとする課題】従来の暗号化されたディジタル情報を記録再生するディジタル情報記録再生装置は、上述のような構成となっているため、例えば、図９において、Ａの時点で記録再生手段８に記録されたディジタル情報は（ｐ１＋ｐ２）の期間再生が可能であるのに対し、Ｂの時点で記録再生手段８に記録されたディジタル情報はｐ２の期間しか再生することができず、さらに、第２の期間の切り替わりの直前に記録再生手段８に記録されたディジタル情報は記録後すぐに第２の期間が切り替わることにより、記憶手段７から出力される第２の暗号化キーが、記録された第２の暗号化情報（ＥＣＭ情報）を解読するのに必要な第２の暗号化キーから、異なる第２の暗号化キーに切り替わってしまうため、記録した情報を再生することができない。

【００１２】また、上述の不都合を回避するために、ディジタル情報の記録時に、記録する第２の暗号化情報（ＥＣＭ情報）を解読するのに必要な第２の暗号化キーを記録再生手段にいっしょに記録しておき、再生時に、記録された第２の暗号化情報（ＥＣＭ情報）をこの記録再生手段に記録された第２の暗号化キーを用いて解読することが考えられるが、暗号解除情報を記録再生手段に記録しておくので、暗号を解読される危険性があり、ディジタル情報の暗号化伝送システムにおけるセキュリティが低下するという問題がある。

【００１３】この発明は、ディジタル情報の暗号化伝送システムにおけるセキュリティを低下させることなく、少なくとも所定の期間は、記録したディジタル情報の再生を可能とできるディジタル情報記録再生装置を提供することを目的とする。

【００１４】

【課題を解決するための手段】上記の課題を解決するために、本発明（請求項１）に係るディジタル情報記録再生装置は、放送局より伝送される、情報を第１の期間ごとに変化する第１の暗号化キーを用いて暗号化した第１の暗号化情報，前記第１の暗号化キーと前記情報の属性情報を第２の期間ごとに変化する第２の暗号化キーによ

り暗号化した第２の暗号化情報，及び次の第２の期間に有効な第２の暗号化キーと個別の契約情報を第３の暗号化キーにより暗号化した第３の暗号化情報を受信する手段と、受信した第３の暗号化情報を前記第３の暗号化キーを用いて暗号を解除して前記第２の暗号化キーと前記個別の契約情報を出力する第１の暗号化解読部と、該第１の暗号化解読部が出力する第２の暗号化キーを次の第２の期間の間保持する第１の記憶手段と、受信した第２の暗号化情報を、一つ前の第２の期間に得られ前記第１の記憶手段に保持された第２の暗号化キーを用いて暗号を解除して前記第１の暗号化キーと前記情報の属性情報を出力する第２の暗号化解読部と、受信した第１の暗号化情報を、前記第２の暗号化解読部より出力され、前記第１の暗号化解読部より出力された個別の契約情報と前記第２の暗号化解読部より出力された情報の属性情報との比較に基づいて与えられる、第１の暗号化キーを用いて暗号を解除して前記情報を得る第３の暗号化解読部と、受信した第１，及び第２の暗号化情報を記録，再生する記録再生手段と、前記第１の記憶手段に保持している第２の暗号化キーを前記第１の記憶手段のデータ変更後一定期間保持する第２の記憶手段とを備え、前記記録再生手段に記録された情報の再生時に、前記第２の暗号化解読部が、前記記録再生手段が再生した第２の暗号化情報を、前記第１または第２の記憶手段に保持された第２の暗号化キーを用いて暗号を解除するようにしたものである。

【００１５】また、本発明（請求項２）に係るディジタル情報記録再生装置は、請求項１記載のディジタル情報記録再生装置において、前記記録再生手段が、第１，第２の暗号化情報とともに記録時の時間情報を記録するものである。

【００１６】また、本発明（請求項３）に係るディジタル情報記録再生装置は、請求項２記載のディジタル情報記録再生装置において、前記記録再生手段に記録された第１，第２の暗号化情報を、該第１，第２の暗号化情報が前記記録再生手段に記録された時から上記第２の記憶手段が第２の暗号化キーを保持する上記一定期間を上限とする所定期間に限り再生可能とする制御手段をさらに備えたものである。

【００１７】また、本発明（請求項４）に係るディジタル情報記録再生装置は、請求項１または請求項３記載のディジタル情報記録再生装置において、前記記録再生手段が、第１，第２の暗号化情報とともに、記録される第２の暗号化情報の解読に有効な第２の暗号化キーが何であるかを示す暗号化キー識別情報を記録するものである。

【００１８】また、本発明（請求項５）に係るディジタル情報記録再生装置は、請求項１ないし請求項４のいずれかに記載のディジタル情報記録再生装置において、前記第１の暗号化解読部，第２の暗号化解読部，第１の記憶手段，及び第２の記憶手段を、ディジタル情報記録再生装置本体に対し着脱自在の電子回路ユニットに搭載したものである。

【００１９】また、本発明（請求項６）に係るディジタル情報記録再生装置は、放送局より伝送される、情報を第１の期間ごとに変化する第１の暗号化キーを用いて暗号化した第１の暗号化情報，前記第１の暗号化キーと前記情報の属性情報を第２の期間ごとに変化する第２の暗号化キーにより暗号化した第２の暗号化情報，及び次の第２の期間に有効な第２の暗号化キーと個別の契約情報を第３の暗号化キーにより暗号化した第３の暗号化情報を受信する手段と、受信した第３の暗号化情報を前記第３の暗号化キーを用いて暗号を解除して前記第２の暗号化キーと前記個別の契約情報を出力する第１の暗号化解読部と、該第１の暗号化解読部が出力する第２の暗号化キーを次の第２の期間の間保持する記憶手段と、受信した第２の暗号化情報を、一つ前の第２の期間に得られ前記第１の記憶手段に保持された第２の暗号化キーを用いて暗号を解除して前記第１の暗号化キーと前記情報の属性情報を出力する第２の暗号化解読部と、受信した第１の暗号化情報を、前記第２の暗号化解読部より出力され、前記第１の暗号化解読部より出力された個別の契約情報と前記第２の暗号化解読部より出力された情報の属性情報との比較に基づいて与えられる、第１の暗号化キーを用いて暗号を解除して前記情報を得る第３の暗号化解読部と、受信した第３の暗号化情報を次の第２の期間の間保持する暗号化情報保持手段と、受信した第１，及び第２の暗号化情報と前記暗号化情報保持手段に保持された一つ前の第２の期間に受信した第３の暗号化情報を記録，再生する記録再生手段とを備えたものである。

【００２０】また、本発明（請求項７）に係るディジタル情報記録再生装置は、請求項６記載のディジタル情報記録再生装置において、上記第３の暗号化解読部が、再生時の直前に取得した個別の契約情報と前記第２の暗号化解読部より出力された情報の属性情報との比較に基づいて与えられる、第１の暗号化キーを用いて、上記記録再生手段が再生する第１の暗号化情報の暗号を解除するものである。

【００２１】また、本発明（請求項８）に係るディジタル情報記録再生装置は、請求項６記載のディジタル情報記録再生装置において、記録時の個別の契約情報を保持する契約情報保持手段をさらに備え、上記第３の暗号化解読部が、上記契約情報保持手段に保持された個別の契約情報と前記第２の暗号化解読部より出力された情報の属性情報との比較に基づいて与えられる、第１の暗号化キーを用いて、上記記録再生手段が再生する第１の暗号化情報の暗号を解除するものである。

【００２２】

【発明の実施の形態】

実施の形態１．以下、本発明の実施の形態１について、

図面を用いて説明する。図１はディジタル情報を暗号化して伝送する際の放送局側における暗号化処理のための構成（放送側）及び本発明の実施の形態１によるディジタル情報記録再生装置の構成を示す図であり、図において図７と同一符号は同一または相当部分である。本実施の形態によるディジタル情報記録再生装置において、第１の記憶手段である記憶手段７は、図７に示す従来例の記憶手段７と同様、図８に示すような、第１の暗号化解読部４が出力する第２の暗号化キーを受け取ってこれを保持する第１の記憶領域７ａと、一つ前の第２の期間に受け取った第２の暗号化キーを保持しこれを第２の暗号化解読部５に対し出力する第２の記憶領域７ｂとを備えている。また、１０は第２の期間が切り替わるタイミングで記憶手段７の第２の記憶領域７ｂに保持されている第２の暗号化キーを受け取り、これを一定期間保持する第２の記憶手段である。

【００２３】次に本実施の形態１によるディジタル情報記録再生装置の動作について説明する。映像情報，音声情報，及びデータを含むディジタル番組情報は第１の暗号化処理部１において第１の暗号化キー（Ｋｓ）を用いて暗号化され、第１の暗号化情報として伝送され、第１の暗号化キー（Ｋｓ）は番組の属性情報とともに第２の暗号化処理部２において第２の暗号化キー（Ｋｗ）を用いて暗号化され、第２の暗号化情報（ＥＣＭ情報）として伝送され、第２の暗号化キー（Ｋｗ）は受信者の個別の契約情報とともに第３の暗号化処理部３において第３の暗号化キーを用いて暗号化され、第３の暗号化情報（ＥＭＭ情報）として伝送される。

【００２４】ディジタル情報記録再生装置側（受信側）では、第１の暗号化解読部４が、あらかじめ与えられている第３の暗号化キーを用いて第３の暗号化情報（ＥＭＭ情報）の暗号化を解読し、第２の暗号化キー，及び個別契約情報を得る。取得された第２の暗号化キーは記憶手段７の第１の記憶領域７ａに保持され、個別契約情報は資格判定部８に入力される。記憶装置７の第１の記憶領域７ａに保持された第２の暗号化キーは第２の期間が切り替わったとき、すなわち、第１の暗号化解読部４から受け取る第２の暗号化キーが変化するタイミングで第２の記憶領域７ｂに移され、それ以前に第２の記憶領域７ｂに保持されていた第２の暗号化キーは第２の記憶手段１０に移され、ここで一定期間保持される。第１の記憶領域７ａと第２の記憶領域７ｂとの間で上述のような保持情報の受け渡しの動作が行なわれることにより、記憶手段７からは、常に、一つ前の第２の期間に取得した第２の暗号化キーが第２の暗号化解読部５に対して出力される。第２の暗号化解読部５は、記憶手段７の第２の記憶領域７ｂに保持された一つ前の第２の期間に受信した第２の暗号化キーを用いて第２の暗号化情報（ＥＣＭ情報）を解読し、第１の暗号化キー（Ｋｓ），及び番組の属性情報を得る。資格判定部８は、第１の暗号化解読部４から得た個別の契約情報と第２の暗号化解読部５から得た番組の属性情報とを比較して、契約者が当該番組を視聴する資格を有するか否かの判定をし、判定結果に応じた制御信号を出力する。スイッチＳＷは資格判定部８からの制御信号に応じて、第２の暗号化解読部で得られた第１の暗号化キー（Ｋｓ）を第３の暗号化解読部６に対して提供，非提供のスイッチングを行なう。また、第３の暗号化解読部６は、第２の暗号化解読部で得られスイッチＳＷを介して提供される第１の暗号化キー（Ｋｓ）を用いて第１の暗号化情報を解読し、番組の情報（映像，音声，データ）を得る。

【００２５】図２は、本実施の形態１によるディジタル情報記録再生装置の動作を説明するためのタイミングチャート図である。図において、上述もしたように、放送局側から第２の暗号化情報（ＥＣＭ情報）に含まれて送信される第１の暗号化キーは、第２の期間の切り替わりとは無関係に第１の期間（数秒）毎に切り替わる。一方、第３の暗号化情報（ＥＭＭ情報）に含まれて放送局側から送信される第２の暗号化キー，及び第２の暗号化情報（ＥＣＭ情報）の解読に有効な第２の暗号化キーは第２の期間毎に切り替わる。図２において、Ｔ１の期間に第２の暗号化情報（ＥＣＭ情報）の解読に有効な第２の暗号化キーはＫｗ１であり、Ｔ２の期間に第２の暗号化情報（ＥＣＭ情報）の解読に有効な第２の暗号化キーはＫｗ２であり、Ｔ３の期間に第２の暗号化情報（ＥＣＭ情報）の解読に有効な第２の暗号化キーはＫｗ３である。また、Ｔ１の期間に放送局側から送信される第３の暗号化情報（ＥＭＭ情報）に含まれて放送局側から送信される第２の暗号化キーはＫｗ２であり、Ｔ２の期間に放送局側から送信される第３の暗号化情報（ＥＭＭ情報）に含まれて放送局側から送信される第２の暗号化キーはＫｗ３であり、Ｔ３の期間に放送局側から送信される第３の暗号化情報（ＥＭＭ情報）に含まれて放送局側から送信される第２の暗号化キーはＫｗ４である。このように、ある第２の期間に放送局側から送信される第２の暗号化情報（ＥＣＭ情報）の解読に有効な第２の暗号化キーは、一つ前の第２の期間に放送局側から送信される第３の暗号化情報（ＥＭＭ情報）に含まれて放送局側から送信される第２の暗号化キーである。そして、記憶手段７が第２の暗号化解読手段５に対し出力する第２の暗号化キーは、Ｔ１の期間はＫｗ１であり、Ｔ２の期間はＫｗ２であり、Ｔ３の期間はＫｗ３である。本実施の形態１によるディジタル情報記録再生装置では、さらに、第２の記憶手段１０が、記憶手段７が出力する第２の暗号化キーが切り替わった後の一定期間、それまで記憶手段７が出力していた第２の暗号化キーを第２の暗号化解読手段５に対し出力する。

【００２６】次に、本実施の形態１によるディジタル情報記録再生装置におけるディジタル情報の記録再生動作について説明する。図示しない記録再生手段制御手段よ

り情報記録の指示を受けて、記録再生手段９は、第１の暗号化情報，及び第２の暗号化情報（ＥＣＭ情報）を記録媒体に記録する。再生時には、再生した第２の暗号化情報（ＥＣＭ情報）を第２の暗号化解読部５に対して出力し、再生した第１の暗号化情報を第３の暗号化解読部６に対して出力する。この再生時に、図示しない記憶手段制御手段は、再生しようとしている情報の第２の暗号化情報が、記憶手段７が出力する第２の暗号化キー、あるいは第２の記憶手段１０が出力する第２の暗号化キーのいずれかによって解読することができるかを判断し、解読可能と判断した場合は、記憶手段７または第２の記憶手段１０が出力する、再生しようとしている情報の第２の暗号化情報の解読に有効な第２の暗号化キーが第２の暗号化解読部５に与えられるように制御する。

【００２７】上記記憶手段制御手段の制御動作の具体例を説明する。この具体例においては、記録再生手段９にディジタル情報を記録する際に、記録される情報の第２の暗号化情報の解読に有効な第２の暗号化キーが何であるかを示す暗号化キー識別情報を同時に記録しておく。この暗号化キー識別情報の記録は、たとえば放送局側で暗号化情報に付加して伝送する番組情報にこの暗号化キー識別情報を含めて伝送するようにすれば、この番組情報を暗号化情報とともに記録することにより、容易に達成できるものである。記録再生手段９が図示しない記録再生手段制御手段より情報再生の指示を受けると、記憶手段制御手段は、再生しようとしている情報の第２の暗号化情報の解読に有効な第２の暗号化キーが何であるかを上記暗号化キー識別情報で認識し、記憶手段７の第２の記憶領域７ｂに保持された第２の暗号化キーおよび第２の記憶手段１０に保持された第２の暗号化キーのいずれかが上記暗号化キー識別情報の示す第２の暗号化キーであるか否かを判断する。記憶手段７の第２の記憶領域７ｂに保持された第２の暗号化キーおよび第２の記憶手段１０に保持された第２の暗号化キーのいずれもが、暗号化キー識別情報の示す第２の暗号化キーでない場合は、図示しない表示手段に、暗号が解読できないことを表示する。記憶手段７の第２の記憶領域７ｂに保持された第２の暗号化キーおよび第２の記憶手段１０に保持された第２の暗号化キーのいずれかが暗号化キー識別情報の示す第２の暗号化キーである場合は、暗号化キー識別情報の示す第２の暗号化キーである方の第２の暗号化キーが第２の暗号化解読手段５に対して出力されるように記憶手段７および第２の記憶手段１０を制御する。

【００２８】例えば、図２において、「ＲＥＣ」で示すタイミングでディジタル情報を記録した場合、記録媒体には、第１の暗号化情報，及び第２の暗号化情報（ＥＣＭ情報）とともに、記録される第２の暗号化情報の解読に有効な第２の暗号化キーがＫｗ２であることを示す暗号化キー識別情報が同時に記録される。記録したディジタル情報の再生時が図２中のＰ１の期間であるときは、記憶手段７の第２の記憶領域７ｂに保持された第２の暗号化キーがＫｗ２であるので、記憶手段制御手段は記憶手段７が第２の暗号化解読手段５に対して第２の暗号化キーを出力するように制御する。また、記録したディジタル情報の再生時が図２中のＰ２の期間であるときは、第２の記憶手段１０に保持された第２の暗号化キーがＫｗ２であるので、記憶手段制御手段は第２の記憶手段１０が第２の暗号化解読手段５に対して第２の暗号化キーを出力するように制御する。

【００２９】このような、本実施の形態１によるディジタル情報記録再生装置では、第２の期間が切り替わる直前にディジタル情報を記録した場合でも、第２の記憶手段に第２の暗号化キーが保持されている一定期間は、記録したディジタル情報の再生を可能とできる。しかも、記録再生手段には、従来のディジタル情報記録再生装置と同様、第１，第２の暗号化情報を記録するものであるので、記録再生手段に暗号化キーそのものを記録する場合のような、ディジタル情報の暗号化伝送システムにおけるセキュリティの低下を招くことはない。

【００３０】このように、本実施の形態１によるディジタル情報記録再生装置では、第１の記憶手段である記憶手段７に保持している第２の暗号化キーを記憶手段７のデータ変更後一定期間保持する第２の記憶手段１０とを備え、第１，第２の暗号化情報を記録，再生する記録再生手段９が、記録した第１，第２の暗号化情報を再生するときに、第２の暗号化情報（ＥＣＭ情報）を解読する第２の暗号化解読部が、前記記録再生手段が再生した第２の暗号化情報を、前記第１または第２の記憶手段に保持された第２の暗号化キーを用いて暗号を解除する構成としたから、ディジタル情報の暗号化伝送システムにおけるセキュリティを低下させることなく、少なくとも所定の期間は、記録したディジタル情報の再生を可能とできるディジタル情報記録再生装置を実現できる。

【００３１】なお、上記説明では、記録再生手段９にディジタル情報を記録する際に、記録される情報の第２の暗号化情報の解読に有効な第２の暗号化キーが何であるかを示す暗号化キー識別情報を同時に記録し、記憶手段制御手段が、この暗号化キー識別情報と記憶手段７の第２の記憶領域７ｂに保持された第２の暗号化キーおよび第２の記憶手段１０に保持された第２の暗号化キーとを比較して、暗号化キー識別情報の示す第２の暗号化キーである方の第２の暗号化キーが第２の暗号化解読手段５に対して出力されるように記憶手段７および第２の記憶手段１０を制御する構成としたが、記録再生手段９にディジタル情報を記録する際に、その記録日時情報を同時に記録し、記憶手段制御手段が、再生時がこの記録日時情報が示す時が属する第２の期間と同じ第２の期間に属するときは記憶手段７に保持された第２の暗号化キーが第２の暗号化解読手段５に対して出力されるように、また、再生時がこの記録日時情報が示す時が属する第２の

期間の次の第２の期間であってかつ第２の記憶手段１０が第２の暗号化キーを保持している一定期間に属するときは第２の記憶手段１０に保持された第２の暗号化キーが第２の暗号化解読手段５に対して出力されるように記憶手段７および第２の記憶手段１０を制御するようにしてもよい。

【００３２】また、本実施の形態１において、第１の暗号化解読部４，第２の暗号化解読部５，記憶手段７，第２の記憶手段１０を、ＩＣカード等、ディジタル情報記録再生装置本体に対し着脱自在な電子回路ユニットに搭載することにより、複数のディジタル情報記録再生装置のうちの一つのディジタル情報記録再生装置において取得した第２の暗号化キーを他のディジタル情報記録再生装置においても使用できるので、長時間の不使用のために当該他のディジタル情報記録再生装置が第２の暗号化キーを取得していない場合にも、情報の再生を行なうことができるディジタル情報記録再生装置を実現することができるものである。

【００３３】実施の形態２．以下、本発明の実施の形態２について、図面を用いて説明する。図３はディジタル情報を暗号化して伝送する際の放送局側における暗号化処理のための構成（放送側）及び本発明の実施の形態２によるディジタル情報記録再生装置の構成を示す図であり、図において図１と同一符号は同一または相当部分である。

【００３４】上述のように、上記実施の形態１によるディジタル情報記録再生装置によれば、第２の期間が切り替わる直前にディジタル情報を記録した場合にも、少なくとも第２の記憶手段１０に第２の暗号化キーが保持されている一定期間は、記録したディジタル情報を再生できる。しかしながら、この実施の形態１によるディジタル情報記録再生装置では、第２の期間のどの時点でディジタル情報を記録したかによって、再生できる期間の長さが異なる。

【００３５】本実施の形態２によるディジタル情報記録再生装置は、実施の形態１によるディジタル情報記録再生装置において、記録再生手段９にディジタル情報を記録する際に、その記録日時情報を同時に記録し、図示しない情報再生制御手段により、前記記録再生手段に記録された第１，第２の暗号化情報を、該第１，第２の暗号化情報が記録再生手段９に記録された時から第２の記憶手段１０が第２の暗号化キーを保持する一定期間を上限とする所定期間に限り再生可能とするように制御する構成としたものである。

【００３６】以下、本実施の形態２によるディジタル情報記録再生装置の記録再生動作について説明する。図４は本実施の形態２によるディジタル情報記録再生装置の再生動作を説明するためのフローチャート図である。

【００３７】図示しない記録再生手段制御手段より情報記録の指示を受けて、記録再生手段９は、第１の暗号化情報，及び第２の暗号化情報（ＥＣＭ情報）を記録媒体に記録する。このとき、記録時の日時情報，及び記録される第２の暗号化情報（ＥＣＭ情報）の解読に有効な第２の暗号化キーが何であるかを示す暗号化キー識別情報を同時に記録する。この暗号化キー識別情報の記録は、たとえば放送局側で暗号化情報に付加して伝送する番組情報にこの暗号化キー識別情報を含めて伝送するようにすれば、この番組情報を暗号化情報とともに記録することにより、容易に達成できるものである。

【００３８】記録再生手段９は図示しない記録再生手段制御手段より情報再生の指示を受けると、再生した第２の暗号化情報（ＥＣＭ情報）を第２の暗号化解読部５に対して出力し、再生した第１の暗号化情報を第３の暗号化解読部６に対して出力する。以降の動作は図４に示すフローチャートに沿って説明する。図示しない再生制御手段は、第２の暗号化解読部５に入力される第２の暗号化情報（ＥＣＭ情報）が、放送を受信した信号であるか、記録再生手段９からの再生信号であるかを検知し（ステップＳ１）、記録再生手段９からの再生信号であるときは、この第２の暗号化情報が記録された時を示す日時情報を再生信号より抽出し、この日時情報と現在日時を比較して、現在日時が記録時から所定の期間（再生可能期間）内であるか否かを判定する（ステップＳ２）。ここで再生可能期間は、第２の記憶手段１０に第２の暗号化キーが保持される一定期間を上限とする所定の期間である。再生制御手段は、再生有効期限内でないと判断したときは図示しない表示手段に期限がすぎていることを表示し（ステップＳ３）、処理を終了し、再生有効期限内であると判断したときは、図示しない記憶手段制御手段に対し、次ステップの実行を行なう指示を出す。記憶手段制御手段は、再生信号より暗号化キー識別情報を抽出し（ステップＳ４）、再生しようとしている情報の第２の暗号化情報の解読に有効な第２の暗号化キーが何であるかを認識し、記憶手段７の第２の記憶領域７ｂに保持された第２の暗号化キーおよび第２の記憶手段１０に保持された第２の暗号化キーのいずれかが上記暗号化キー識別情報の示す第２の暗号化キーであるか否かを判断する（ステップＳ５）。記憶手段７の第２の記憶領域７ｂに保持された第２の暗号化キーおよび第２の記憶手段１０に保持された第２の暗号化キーのいずれもが、暗号化キー識別情報の示す第２の暗号化キーでない場合は、図示しない表示手段に、暗号が解読できないことを表示し（ステップＳ６）、処理を終了する。記憶手段７の第２の記憶領域７ｂに保持された第２の暗号化キーおよび第２の記憶手段１０に保持された第２の暗号化キーのいずれかが暗号化キー識別情報の示す第２の暗号化キーである場合は、暗号化キー識別情報の示す第２の暗号化キーである方の第２の暗号化キーが第２の暗号化解読手段５に対して出力されるように記憶手段７および第２の記憶手段１０を制御する。第２の暗号化解読手段

５はこの第２の暗号化キーを用いて第２の暗号化情報（ＥＣＭ情報）を解読し、第１の暗号化キーと番組の属性情報を出力する（ステップＳ７）。資格判定部８は第２の暗号化解読手段５が出力する番組の属性情報と個別の契約情報とを比較してユーザが当該番組の視聴資格を有するか否かを判定し（ステップＳ８）、番組のデコードが可能か否かを判断する（ステップＳ９）。デコード不可能と判断した場合は第１の暗号化キーが第３の暗号化解読部６に提供されないようにスイッチＳＷを制御するとともに、図示しない表示手段に、暗号が解読できないことを表示し（ステップＳ６）、処理を終了する。一方、デコード可能と判断した場合は第１の暗号化キーが第３の暗号化解読部６に提供されるようにスイッチＳＷを制御する。第３の暗号化解読部６は第２の暗号化解読手段５からスイッチＳＷを介して入力される第１の暗号化キーを用いて記録再生部９が再生する第１の暗号化情報の暗号を解読し（ステップＳ１０）、番組の情報（映像，音声，データ）を得る。

【００３９】このように、本実施の形態２によるディジタル情報記録再生装置では、第１の記憶手段である記憶手段７に保持している第２の暗号化キーを記憶手段７のデータ変更後一定期間保持する第２の記憶手段１０を備え、第１，第２の暗号化情報を記録，再生する記録再生手段９が、記録した第１，第２の暗号化情報を再生するときに、第２の暗号化情報（ＥＣＭ情報）を解読する第２の暗号化解読部が、前記記録再生手段が再生した第２の暗号化情報を、前記第１または第２の記憶手段に保持された第２の暗号化キーを用いて暗号を解除する構成とするとともに、記録再生手段９にディジタル情報を記録する際に、その記録日時情報を同時に記録し、図示しない情報再生制御手段により、前記記録再生手段に記録された第１，第２の暗号化情報を、該第１，第２の暗号化情報が記録再生手段９に記録された時から第２の記憶手段１０が第２の暗号化キーを保持する一定期間を上限とする所定期間に限り再生可能とするように制御する構成としたから、ディジタル情報の暗号化伝送システムにおけるセキュリティを低下させることなく、第２の期間のどの時点でディジタル情報を記録した場合であっても、一律に一定期間、記録したディジタル情報の再生を可能とできるディジタル情報記録再生装置を実現できる。

【００４０】なお、上記説明では、記録再生手段９にディジタル情報を記録する際に、記録される情報の第２の暗号化情報の解読に有効な第２の暗号化キーが何であるかを示す暗号化キー識別情報を同時に記録し、記憶手段制御手段が、この暗号化キー識別情報と記憶手段７の第２の記憶領域７ｂに保持された第２の暗号化キーおよび第２の記憶手段１０に保持された第２の暗号化キーとを比較して、暗号化キー識別情報の示す第２の暗号化キーである方の第２の暗号化キーが第２の暗号化解読手段５に対して出力されるように記憶手段７および第２の記憶



手段１０を制御する構成としたが、記憶手段制御手段が、再生時が、記録日時情報が示す時が属する第２の期間と同じ第２の期間に属するときは記憶手段７に保持された第２の暗号化キーが第２の暗号化解読手段５に対して出力されるように、また、再生時が、記録日時情報が示す時が属する第２の期間の次の第２の期間に属するときは第２の記憶手段１０に保持された第２の暗号化キーが第２の暗号化解読手段５に対して出力されるように記憶手段７および第２の記憶手段１０を制御するようにしてもよい。

【００４１】また、本実施の形態２において、第１の暗号化解読部４，第２の暗号化解読部５，記憶手段７，第２の記憶手段１０を、ＩＣカード等、ディジタル情報記録再生装置本体に対し着脱自在な電子回路ユニットに搭載することにより、複数のディジタル情報記録再生装置のうちの一つのディジタル情報記録再生装置において取得した第２の暗号化キーを他のディジタル情報記録再生装置においても使用できるので、長時間の不使用のために当該他のディジタル情報記録再生装置が第２の暗号化キーを取得していない場合にも、情報の再生を行なうことができるディジタル情報記録再生装置を実現することができるものである。

【００４２】実施の形態３．以下、本発明の実施の形態３について、図面を用いて説明する。図５はディジタル情報を暗号化して伝送する際の放送局側における暗号化処理のための構成（放送側）及び本発明の実施の形態２によるディジタル情報記録再生装置の構成を示す図であり、図において図１と同一符号は同一または相当部分である。また、１１は受信した第３の暗号化情報（ＥＭＭ情報）を次の第２の期間の間保持するＥＭＭ情報保持手段である。

【００４３】次に本実施の形態３によるディジタル情報記録再生装置の動作について説明する。本実施の形態３によるディジタル情報記録再生装置の通常のディジタル情報の受信，表示動作は、従来のディジタル情報記録再生装置と同様である。

【００４４】すなわち、第１の暗号化解読部４が、あらかじめ与えられている第３の暗号化キーを用いて受信した第３の暗号化情報（ＥＭＭ情報）の暗号化を解読し、第２の暗号化キー，及び個別契約情報を得る。取得された第２の暗号化キーは記憶手段７の第１の記憶領域７ａに保持され、個別契約情報は資格判定部８に入力される。記憶装置７の第１の記憶領域７ａに保持された第２の暗号化キーは第２の期間が切り替わったとき、すなわち、第１の暗号化解読部４から受け取る第２の暗号化キーが変化するタイミングで第２の記憶領域７ｂに移され、それ以前に第２の記憶領域７ｂに保持されていた第２の暗号化キーは消去される。第１の記憶領域７ａと第２の記憶領域７ｂとの間で上述のような保持情報の受け渡しの動作が行なわれることにより、記憶手段７から

は、常に、一つ前の第２の期間に取得した第２の暗号化キーが第２の暗号化解読部５に対して出力される。第２の暗号化解読部５は、記憶手段７の第２の記憶領域７ｂに保持された一つ前の第２の期間に受信した第２の暗号化キーを用いて第２の暗号化情報（ＥＣＭ情報）を解読し、第１の暗号化キー（Ｋｓ），及び番組の属性情報を得る。資格判定部８は、第１の暗号化解読部４から得た個別の契約情報と第２の暗号化解読部５から得た番組の属性情報とを比較して、契約者が当該番組を視聴する資格を有するか否かの判定をし、判定結果に応じた制御信号を出力する。スイッチＳＷは資格判定部８からの制御信号に応じて、第２の暗号化解読部で得られた第１の暗号化キー（Ｋｓ）を第３の暗号化解読部６に対して提供，非提供のスイッチングを行なう。また、第３の暗号化解読部６は、第２の暗号化解読部で得られスイッチＳＷを介して提供される第１の暗号化キー（Ｋｓ）を用いて第１の暗号化情報を解読し、番組の情報（映像，音声，データ）を得る。

【００４５】図６は、本実施の形態３によるディジタル情報記録再生装置の動作を説明するためのタイミングチャート図である。図において、放送局側から第２の暗号化情報（ＥＣＭ情報）に含まれて送信される第１の暗号化キーは、第２の期間の切り替わりとは無関係に第１の期間（数秒）毎に切り替わる。一方、第３の暗号化情報（ＥＭＭ情報）に含まれて放送局側から送信される第２の暗号化キー，及び第２の暗号化情報（ＥＣＭ情報）の解読に有効な第２の暗号化キーは第２の期間毎に切り替わる。図２において、Ｔ１の期間に第２の暗号化情報（ＥＣＭ情報）の解読に有効な第２の暗号化キーはＫｗ１であり、Ｔ２の期間に第２の暗号化情報（ＥＣＭ情報）の解読に有効な第２の暗号化キーはＫｗ２であり、Ｔ３の期間に第２の暗号化情報（ＥＣＭ情報）の解読に有効な第２の暗号化キーはＫｗ３である。また、Ｔ１の期間に放送局側から送信される第３の暗号化情報（ＥＭＭ情報）に含まれて放送局側から送信される第２の暗号化キーはＫｗ２であり、Ｔ２の期間に放送局側から送信される第３の暗号化情報（ＥＭＭ情報）に含まれて放送局側から送信される第２の暗号化キーはＫｗ３であり、Ｔ３の期間に放送局側から送信される第３の暗号化情報（ＥＭＭ情報）に含まれて放送局側から送信される第２の暗号化キーはＫｗ４である。このように、ある第２の期間に放送局側から送信される第２の暗号化情報（ＥＣＭ情報）の解読に有効な第２の暗号化キーは、一つ前の第２の期間に放送局側から送信される第３の暗号化情報（ＥＭＭ情報）に含まれて放送局側から送信される第２の暗号化キーである。

【００４６】また、本実施の形態３によるディジタル情報記録再生装置では、受信した第３の暗号化情報（ＥＭＭ情報）を、ＥＭＭ情報保持手段１１が、次の第２の期間の間保持する。すなわち、図５において、Ｔ１の期間



は、これに含まれる第２の暗号化キーがＫｗ１であるＥＭＭ情報がＥＭＭ情報保持手段１１に保持され、Ｔ２の期間、これに含まれる第２の暗号化キーがＫｗ２であるＥＭＭ情報がはＥＭＭ情報保持手段１１に保持され、Ｔ３の期間は、これに含まれる第２の暗号化キーがＫｗ３であるＥＭＭ情報がＥＭＭ情報保持手段１１に保持される。

【００４７】次に、本実施の形態３によるディジタル情報記録再生装置におけるディジタル情報の記録再生動作について説明する。図示しない記録再生手段制御手段より情報記録の指示を受けて、記録再生手段９は、受信した第１の暗号化情報，第２の暗号化情報（ＥＣＭ情報），及びＥＭＭ情報保持手段に１１に保持された第３の暗号化情報（ＥＭＭ情報）を記録媒体に記録する。すなわち、記録媒体には、受信した第１の暗号化情報，第２の暗号化情報（ＥＣＭ情報）とともに、当該受信した第２の暗号化情報（ＥＣＭ情報）の解読に有効な第２の暗号化キーが暗号化されて含まれる第３の暗号化情報（ＥＭＭ情報）が記録されることとなる。再生時に記録再生手段９は、再生した第３の暗号化情報（ＥＭＭ情報）を第１の暗号化解読部４に対して出力し、再生した第２の暗号化情報（ＥＣＭ情報）を第２の暗号化解読部５に対して出力し、再生した第１の暗号化情報を第３の暗号化解読部６に対して出力する。第１の暗号化解読部４は、通常の動作と同様に、第３の暗号化キーを用いて、記録再生手段９が再生した第３の暗号化情報（ＥＭＭ情報）を解読し、第２の暗号化キーを出力する。なお、個別の契約情報については、受信した第３の暗号化情報（ＥＭＭ情報）を解読して得られた契約情報のうち、再生時の直前に得られたものを用いる。ここで出力される第２の暗号化キーは記録再生手段９が再生する第２の暗号化情報（ＥＣＭ情報）の解読に有効な第２の暗号化キーである。第２の暗号化解読部５は、記録情報の再生時には、記憶手段７が出力する第２の暗号化キーではなく、第１の暗号化解読部４が出力する第２の暗号化キーを用いるように制御される。従って、第２の暗号化解読部５は、第１の暗号化解読部４が出力する、記録再生手段９が再生する第２の暗号化情報（ＥＣＭ情報）の解読に有効な第２の暗号化キーを用いて、入力される第２の暗号化情報（ＥＣＭ情報）の解読を行なうことができる。以降は通常の動作と同様に、第２の暗号化解読部で得られスイッチＳＷを介して提供される第１の暗号化キー（Ｋｓ）を用いて第１の暗号化情報を解読し、番組の情報（映像，音声，データ）を得る。

【００４８】このように、本実施の形態３によるディジタル情報記録再生装置では、受信し第３の暗号化情報（ＥＭＭ情報）を次の第２の期間の間保持するＥＭＭ情報保持手段１１を備え、記録再生手段９が、受信した第１，第２の暗号化情報とともに上記ＥＭＭ情報保持手段に保持された第３の暗号化情報を記録する構成としたか

ら、ディジタル情報の暗号化伝送システムにおけるセキュリティを低下させることなく、記録したディジタル情報を確実に再生可能とできるディジタル情報記録再生装置を実現できる。

【００４９】なお、上記実施の形態３では、個別の契約情報については、再生時の直前に取得したものを資格判定に用いる構成としたが、情報の記録時の個別の契約情報を保持する手段を設け、再生時にこの保持された契約情報を資格判定部８に入力する構成としてもよい。このような構成とすれば、再生時直前に取得した個別の契約情報が、記録された情報の視聴を不可とする内容となっている場合でも、記録された情報の再生を行なうことができ、個別の契約情報の変更によって、記録した情報が再生できないという不都合が生じることを回避できる。

【００５０】

【発明の効果】以上のように、本発明（請求項１）に係るディジタル情報記録再生装置によれば、放送局より伝送される、情報を第１の期間ごとに変化する第１の暗号化キーを用いて暗号化した第１の暗号化情報，前記第１の暗号化キーと前記情報の属性情報を第２の期間ごとに変化する第２の暗号化キーにより暗号化した第２の暗号化情報，及び次の第２の期間に有効な第２の暗号化キーと個別の契約情報を第３の暗号化キーにより暗号化した第３の暗号化情報を受信する手段と、受信した第３の暗号化情報を前記第３の暗号化キーを用いて暗号を解除して前記第２の暗号化キーと前記個別の契約情報を出力する第１の暗号化解読部と、該第１の暗号化解読部が出力する第２の暗号化キーを次の第２の期間の間保持する第１の記憶手段と、受信した第２の暗号化情報を、一つ前の第２の期間に得られ前記第１の記憶手段に保持された第２の暗号化キーを用いて暗号を解除して前記第１の暗号化キーと前記情報の属性情報を出力する第２の暗号化解読部と、受信した第１の暗号化情報を、前記第２の暗号化解読部より出力され、前記第１の暗号化解読部より出力された個別の契約情報と前記第２の暗号化解読部より出力された情報の属性情報との比較に基づいて与えられる、第１の暗号化キーを用いて暗号を解除して前記情報を得る第３の暗号化解読部と、受信した第１，及び第２の暗号化情報を記録，再生する記録再生手段と、前記第１の記憶手段に保持している第２の暗号化キーを前記第１の記憶手段のデータ変更後一定期間保持する第２の記憶手段とを備え、前記記録再生手段に記録された情報の再生時に、前記第２の暗号化解読部が、前記記録再生手段が再生した第２の暗号化情報を、前記第１または第２の記憶手段に保持された第２の暗号化キーを用いて暗号を解除する構成としたから、ディジタル情報の暗号化伝送システムにおけるセキュリティを低下させることなく、少なくとも所定の期間は、記録したディジタル情報の再生を可能とできるディジタル情報記録再生装置を実現できる効果がある。



【００５１】また、本発明（請求項２）に係るディジタル情報記録再生装置によれば、請求項１記載のディジタル情報記録再生装置において、前記記録再生手段が、第１，第２の暗号化情報とともに記録時の時間情報を記録するものとしたから、再生時が属する第２の期間と記録時が属する第２の期間の比較に基づいて、前記第１または第２の記憶手段に保持された第２の暗号化キーのいずれかを用いて記録再生手段が再生した第２の暗号化情報の暗号を解除でき、ディジタル情報の暗号化伝送システムにおけるセキュリティを低下させることなく、少なくとも所定の期間は、記録したディジタル情報の再生を可能とできるディジタル情報記録再生装置を実現できる効果がある。

【００５２】また、本発明（請求項３）に係るディジタル情報記録再生装置によれば、請求項２記載のディジタル情報記録再生装置において、前記記録再生手段に記録された第１，第２の暗号化情報を、該第１，第２の暗号化情報が前記記録再生手段に記録された時から上記第２の記憶手段が第２の暗号化キーを保持する上記一定期間を上限とする所定期間に限り再生可能とする制御手段をさらに備えた構成としたから、ディジタル情報の暗号化伝送システムにおけるセキュリティを低下させることなく、第２の期間のどの時点でディジタル情報を記録した場合であっても、一律に一定期間、記録したディジタル情報の再生を可能とできるディジタル情報記録再生装置を実現できる効果がある。

【００５３】また、本発明（請求項４）に係るディジタル情報記録再生装置によれば、請求項１または請求項３記載のディジタル情報記録再生装置において、前記記録再生手段が、第１，第２の暗号化情報とともに、記録される第２の暗号化情報の解読に有効な第２の暗号化キーが何であるかを示す暗号化キー識別情報を記録するようにしたから、前記第１または第２の記憶手段に保持された第２の暗号化キーのうち暗号化キー識別情報が示す第２の暗号化キーを用いて記録再生手段が再生した第２の暗号化情報の暗号を解除でき、ディジタル情報の暗号化伝送システムにおけるセキュリティを低下させることなく、第２の期間のどの時点でディジタル情報を記録した場合であっても、一律に一定期間、記録したディジタル情報の再生を可能とできるディジタル情報記録再生装置を実現できる効果がある。

【００５４】また、本発明（請求項５）に係るディジタル情報記録再生装置によれば、請求項１ないし請求項４のいずれかに記載のディジタル情報記録再生装置において、前記第１の暗号化解読部，第２の暗号化解読部，第１の記憶手段，及び第２の記憶手段を、ディジタル情報記録再生装置本体に対し着脱自在の電子回路ユニットに搭載したから、請求項１ないし請求項４に係る発明のそれぞれによる効果に加えて、複数のディジタル情報記録再生装置のうちの一つのディジタル情報記録再生装置に

おいて取得した第２の暗号化キーを他のディジタル情報記録再生装置においても使用でき、長時間の不使用のために当該他のディジタル情報記録再生装置が第２の暗号化キーを取得していない場合にも、情報の再生を行なうことができるディジタル情報記録再生装置を実現することができる効果がある。

【００５５】また、本発明（請求項６）に係るディジタル情報記録再生装置によれば、放送局より伝送される、情報を第１の期間ごとに変化する第１の暗号化キーを用いて暗号化した第１の暗号化情報，前記第１の暗号化キーと前記情報の属性情報を第２の期間ごとに変化する第２の暗号化キーにより暗号化した第２の暗号化情報，及び次の第２の期間に有効な第２の暗号化キーと個別の契約情報を第３の暗号化キーにより暗号化した第３の暗号化情報を受信する手段と、受信した第３の暗号化情報を前記第３の暗号化キーを用いて暗号を解除して前記第２の暗号化キーと前記個別の契約情報を出力する第１の暗号化解読部と、該第１の暗号化解読部が出力する第２の暗号化キーを次の第２の期間の間保持する記憶手段と、受信した第２の暗号化情報を、一つ前の第２の期間に得られ前記第１の記憶手段に保持された第２の暗号化キーを用いて暗号を解除して前記第１の暗号化キーと前記情報の属性情報を出力する第２の暗号化解読部と、受信した第１の暗号化情報を、前記第２の暗号化解読部より出力され、前記第１の暗号化解読部より出力された個別の契約情報と前記第２の暗号化解読部より出力された情報の属性情報との比較に基づいて与えられる、第１の暗号化キーを用いて暗号を解除して前記情報を得る第３の暗号化解読部と、受信した第３の暗号化情報を次の第２の期間の間保持する暗号化情報保持手段と、受信した第１，及び第２の暗号化情報と前記暗号化情報保持手段に保持された一つ前の第２の期間に受信した第３の暗号化情報を記録，再生する記録再生手段とを備えた構成としたから、ディジタル情報の暗号化伝送システムにおけるセキュリティを低下させることなく、記録したディジタル情報を確実に再生可能とできるディジタル情報記録再生装置を実現できる効果がある。

【００５６】また、本発明（請求項７）に係るディジタル情報記録再生装置によれば、請求項６に記載のディジタル情報記録再生装置において、上記第３の暗号化解読部が、再生時の直前に取得した個別の契約情報と前記第２の暗号化解読部より出力された情報の属性情報との比較に基づいて与えられる、第１の暗号化キーを用いて、上記記録再生手段が再生する第１の暗号化情報の暗号を解除する構成としたから、ディジタル情報の暗号化伝送システムにおけるセキュリティを低下させることなく、記録したディジタル情報を、再生時の契約情報により再生可能な番組については、再生可能とできるディジタル情報記録再生装置を実現できる効果がある。

【００５７】また、本発明（請求項８）に係るディジタル情報記録再生装置によれば、請求項６記載のディジタル情報記録再生装置において、記録時の個別の契約情報を保持する契約情報保持手段をさらに備え、上記第３の暗号化解読部が、上記契約情報保持手段に保持された個別の契約情報と前記第２の暗号化解読部より出力された情報の属性情報との比較に基づいて与えられる、第１の暗号化キーを用いて、上記記録再生手段が再生する第１の暗号化情報の暗号を解除する構成としたから、再生時直前に取得した個別の契約情報が、記録された情報の視聴を不可とする内容となっている場合でも、記録された情報の再生を行なうことができ、個別の契約情報の変更によって、記録した情報が再生できないという不都合が生じることを回避できる効果がある。

【図面の簡単な説明】

【図１】ディジタル情報を暗号化して伝送する際の放送局側における暗号化処理のための構成（放送側）及び本発明の実施の形態１によるディジタル情報記録再生装置の構成を示す図である。

【図２】本発明の実施の形態１によるディジタル情報記録再生装置の動作を説明するためのタイミングチャート図である。

【図３】ディジタル情報を暗号化して伝送する際の放送局側における暗号化処理のための構成（放送側）及び本発明の実施の形態２によるディジタル情報記録再生装置の構成を示す図である。

【図４】本発明の実施の形態２によるディジタル情報記録再生装置の再生動作を説明するためのフローチャート図である。

【図５】ディジタル情報を暗号化して伝送する際の放送局側における暗号化処理のための構成（放送側）及び本発明の実施の形態３によるディジタル情報記録再生装置の構成を示す図である。

【図６】本発明の実施の形態３によるディジタル情報記録再生装置の動作を説明するためのタイミングチャート図である。

【図７】ディジタル情報を暗号化して伝送する際の放送局側における暗号化処理のための構成（放送側）及び従来のディジタル情報記録再生装置の構成を示す図である。

【図８】記憶手段７の構成を示す図である。

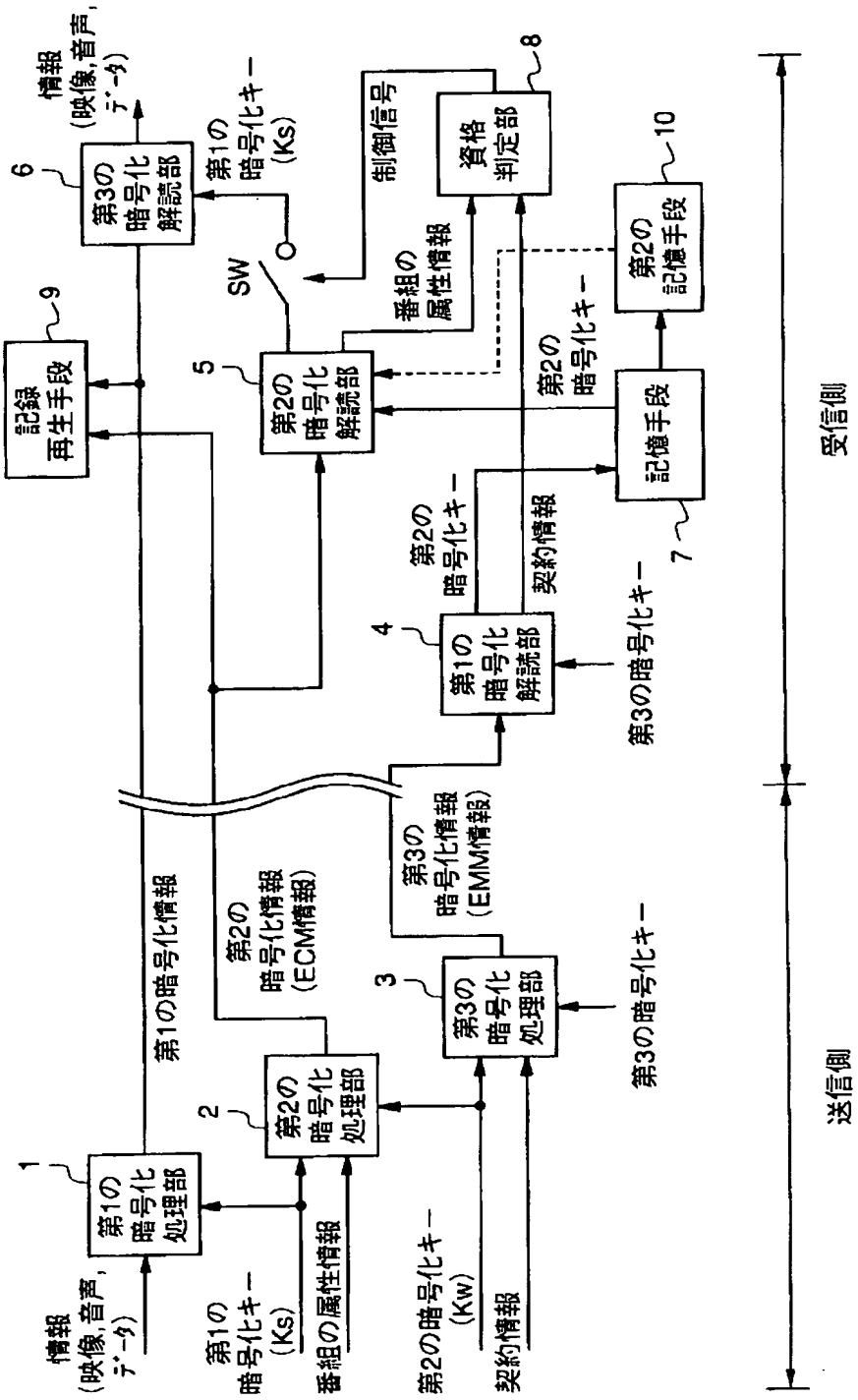
【図９】従来のディジタル情報記録再生装置の動作を説明するためのタイミングチャート図である。

【符号の説明】

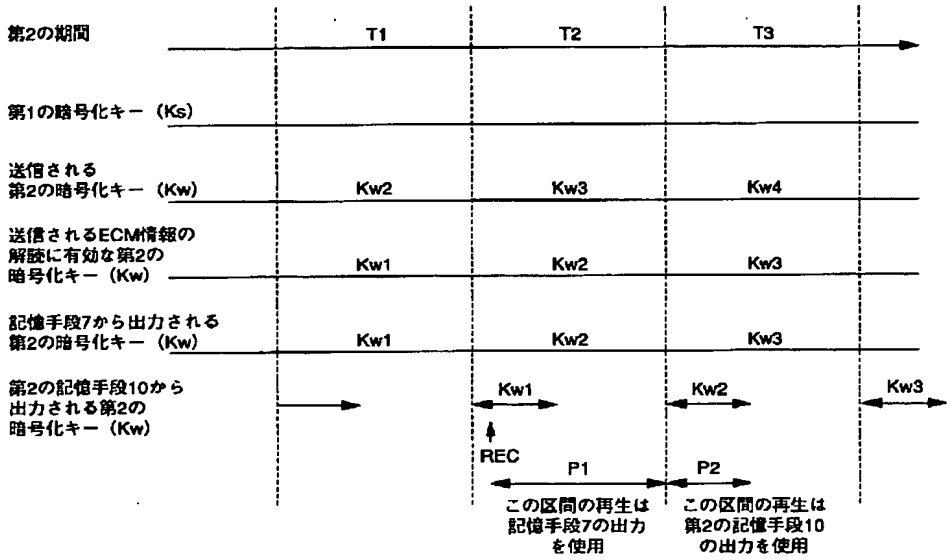
１　第１の暗号化処理部
２　第２の暗号化処理部
３　第３の暗号化処理部
４　第１の暗号化解読部
５　第２の暗号化解読部
６　第３の暗号化解読部
７　記憶手段

７ａ　第１の記憶領域
７ｂ　第２の記憶領域
８　資格判定部
＊９　記録再生手段
１０　第２の記憶手段
＊　１１　ＥＭＭ情報保持手段

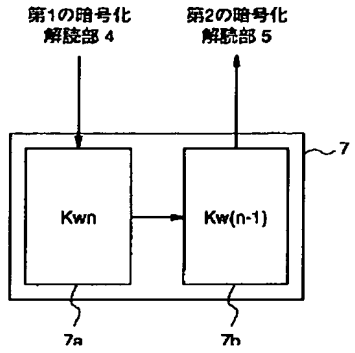
【図１】



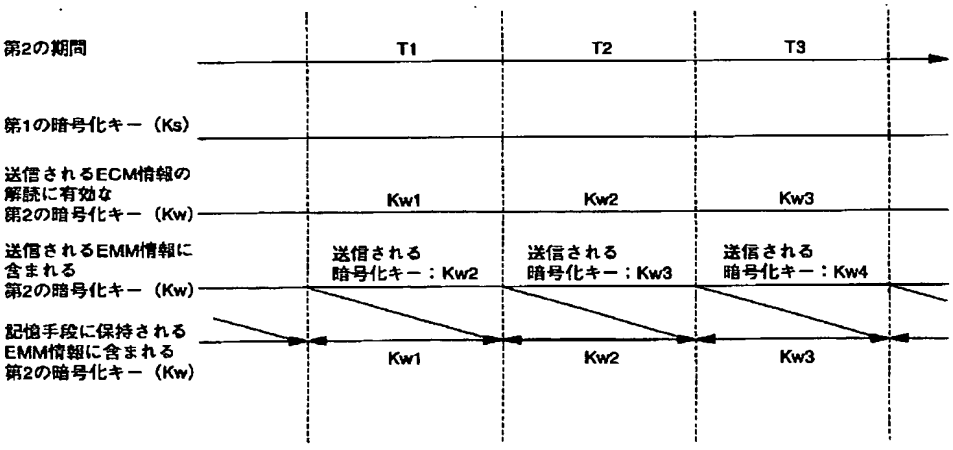
【図２】


第2の期間
T1
T2
T3
第1の暗号化キー（Ks）
送信される
第2の暗号化キー（Kw）
Kw2
Kw3
Kw4
送信されるECM情報の
解読に有効な第2の
暗号化キー（Kw）
Kw1
Kw2
Kw3
記憶手段7から出力される
第2の暗号化キー（Kw）
Kw1
Kw2
Kw3
第2の記憶手段10から
出力される第2の
暗号化キー（Kw）
Kw1
Kw2
Kw3
REC
P1
P2
この区間の再生は
記憶手段7の出力
を使用
この区間の再生は
第2の記憶手段10
の出力を使用

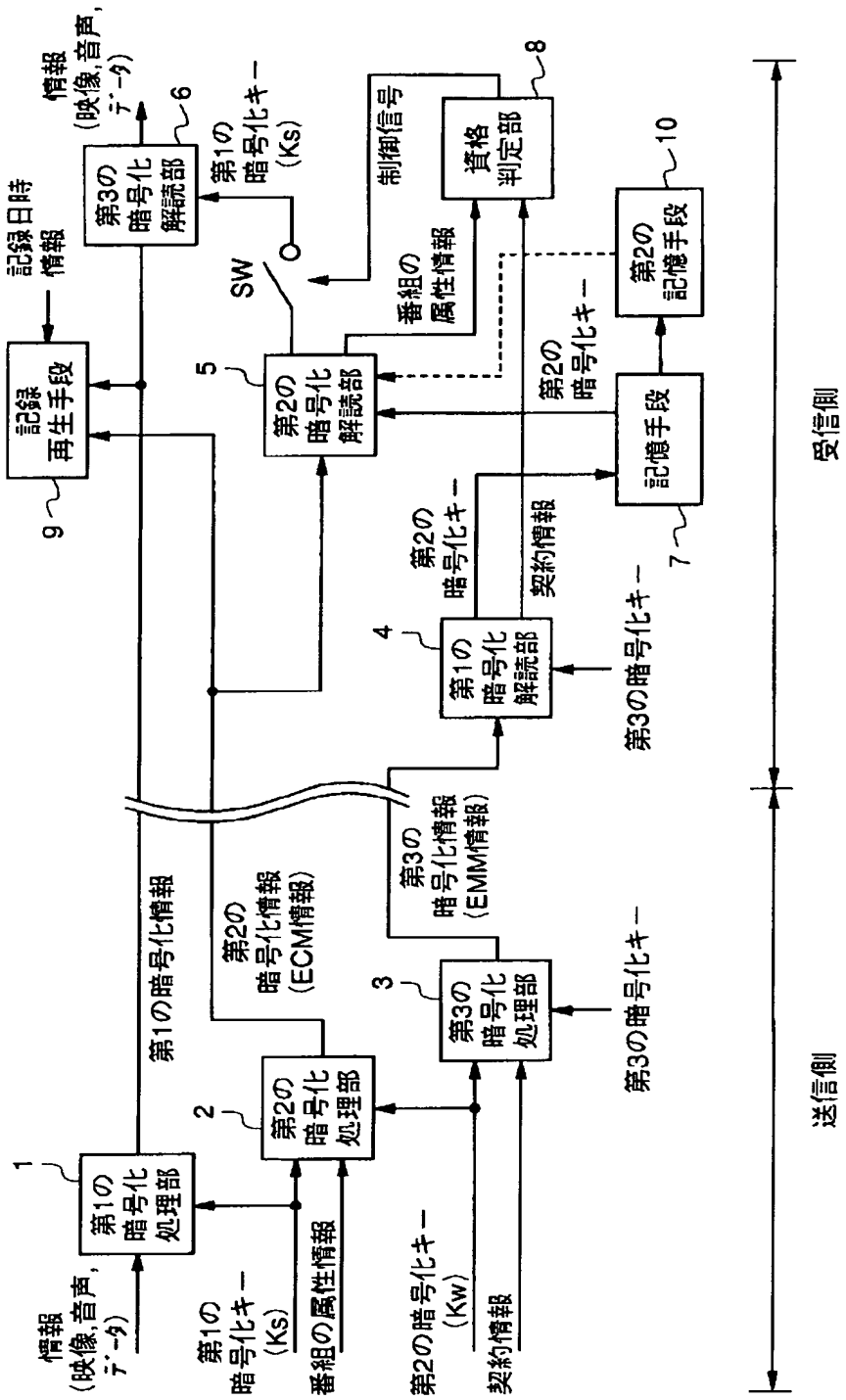
【図８】


第1の暗号化
解読部 4
第2の暗号化
解読部 5
7
Kwn
Kw(n-1)
7a
7b

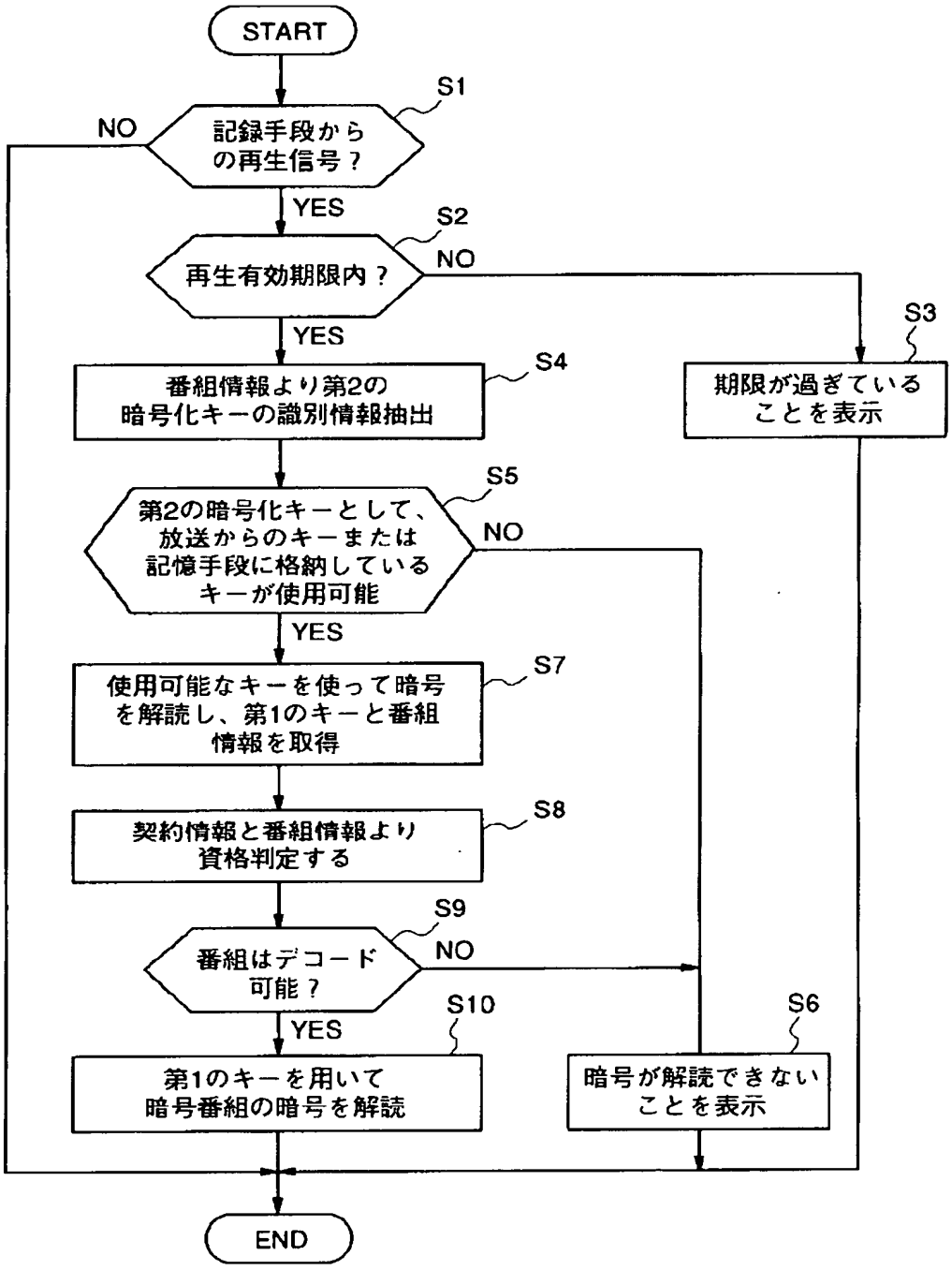
【図６】


第2の期間
T1
T2
T3
第1の暗号化キー（Ks）
送信されるECM情報の
解読に有効な
第2の暗号化キー（Kw）
Kw1
Kw2
Kw3
送信されるEMM情報に
含まれる
第2の暗号化キー（Kw）
送信される
暗号化キー：Kw2
送信される
暗号化キー：Kw3
送信される
暗号化キー：Kw4
記憶手段に保持される
EMM情報に含まれる
第2の暗号化キー（Kw）
Kw1
Kw2
Kw3

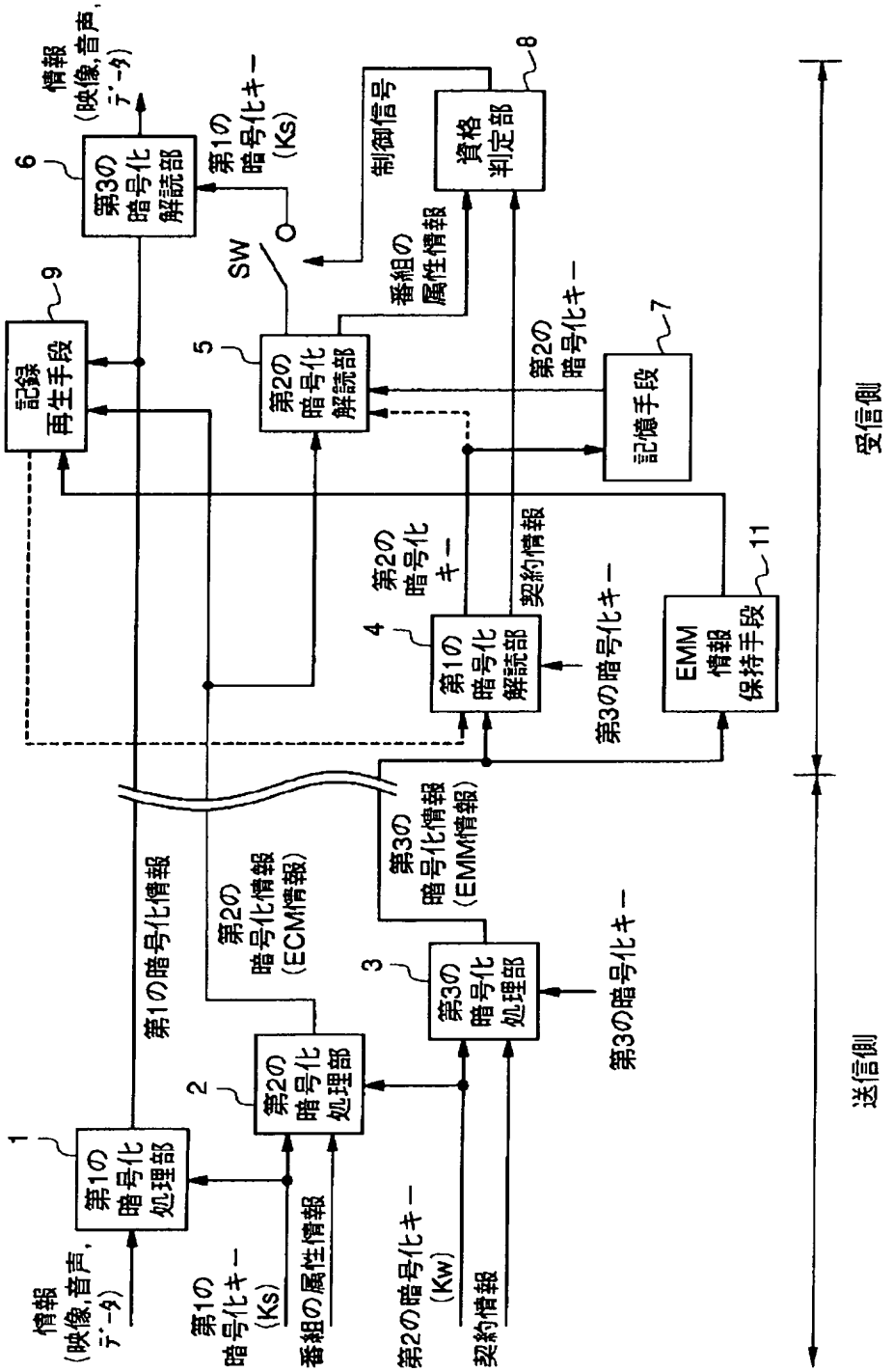
【図３】


情報（映像,音声,データ）
第1の暗号化処理部
1
第1の暗号化情報
第2の暗号化処理部
2
第2の暗号化情報（ECM情報）
第3の暗号化処理部
3
第3の暗号化情報（EMM情報）
第1の暗号化解読部
4
第2の暗号化解読部
5
第3の暗号化解読部
6
記録再生手段
9
記憶手段
7
第2の記憶手段
10
資格判定部
8
第1の暗号化キー（Ks）
第2の暗号化キー（Kw）
第3の暗号化キー
番組の属性情報
契約情報
制御信号
SW
記録日時情報
送信側
受信側

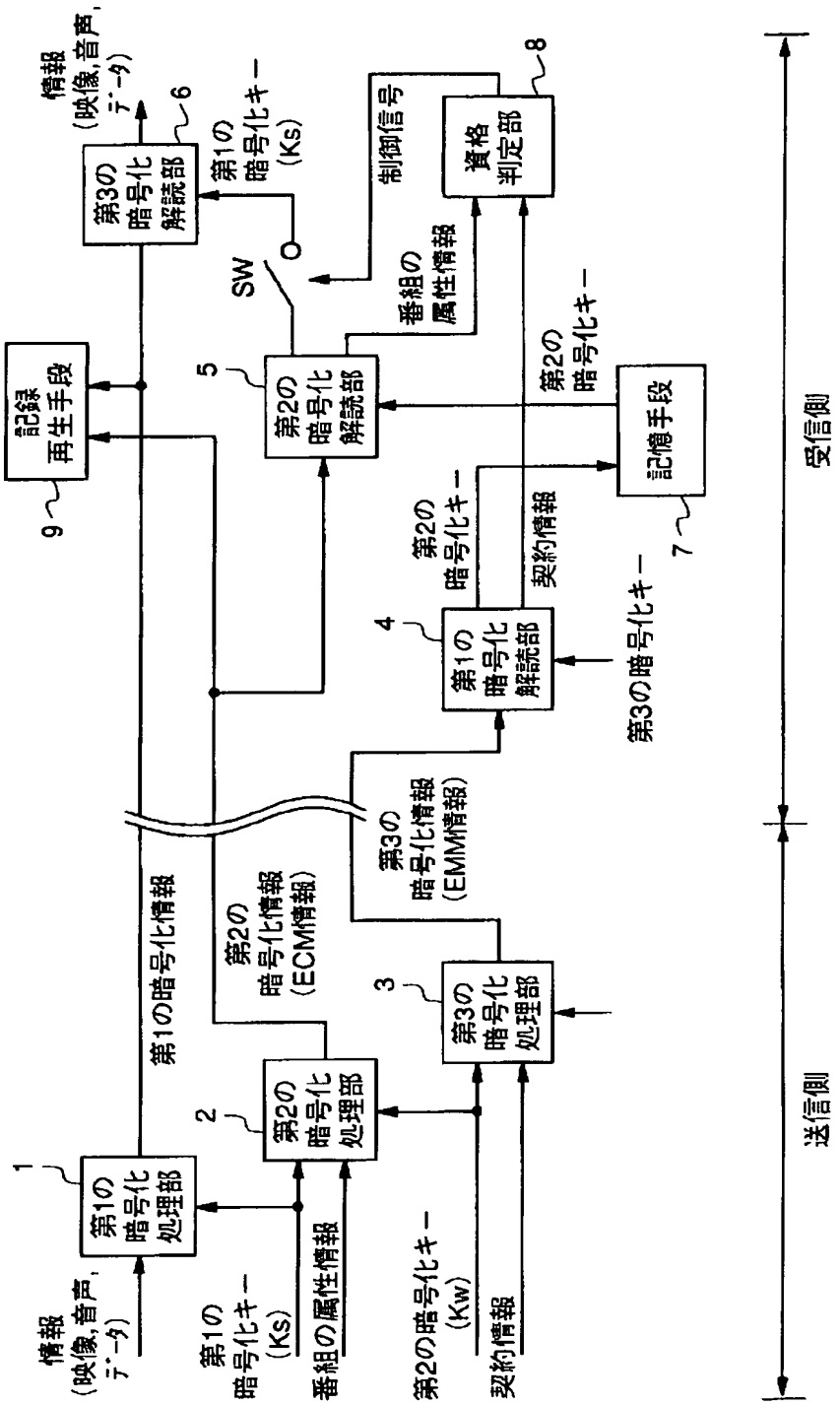
【図４】


START
S1
記録手段から
の再生信号？
NO
YES
S2
再生有効期限内？
NO
YES
S3
期限が過ぎている
ことを表示
S4
番組情報より第2の
暗号化キーの識別情報抽出
S5
第2の暗号化キーとして、
放送からのキーまたは
記憶手段に格納している
キーが使用可能
NO
YES
S7
使用可能なキーを使って暗号
を解読し、第1のキーと番組
情報を取得
S8
契約情報と番組情報より
資格判定する
S9
番組はデコード
可能？
NO
YES
S10
第1のキーを用いて
暗号番組の暗号を解読
S6
暗号が解読できない
ことを表示
END

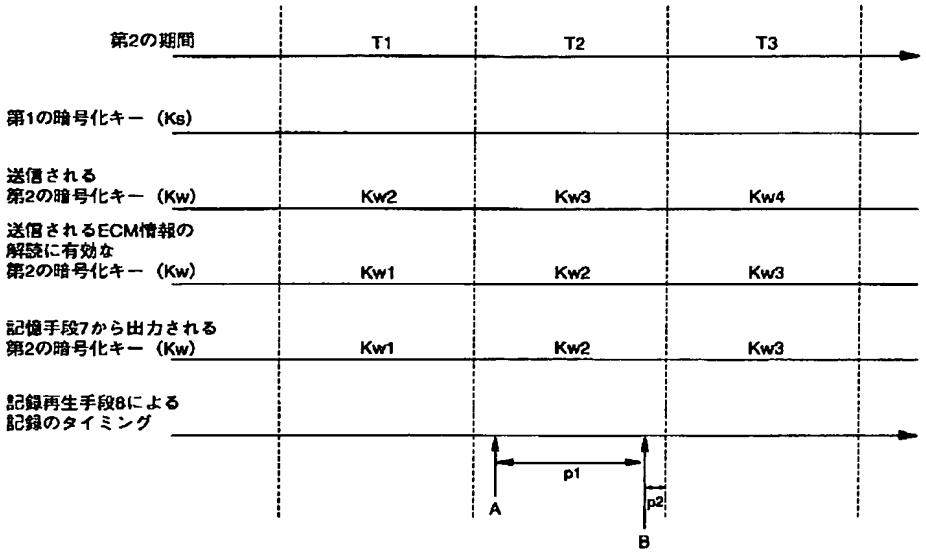
【図５】


情報（映像，音声，データ）
第1の暗号化処理部
第2の暗号化処理部
第3の暗号化処理部
第1の暗号化解読部
第2の暗号化解読部
第3の暗号化解読部
第1の暗号化情報
第2の暗号化情報（ECM情報）
第3の暗号化情報（EMM情報）
第1の暗号化キー（Ks）
番組の属性情報
第2の暗号化キー（Kw）
契約情報
第3の暗号化キー
制御信号
SW
資格判定部
記録再生手段
記憶手段
EMM情報保持手段
受信側
送信側

【図７】


情報（映像，音声，データ）
第1の暗号化処理部
1
第1の暗号化情報
第2の暗号化処理部
2
第2の暗号化情報（ECM情報）
第3の暗号化処理部
3
第3の暗号化情報（EMM情報）
第1の暗号化解読部
4
第2の暗号化解読部
5
第3の暗号化解読部
6
記憶手段
7
資格判定部
8
記録再生手段
9
第1の暗号化キー（Ks）
番組の属性情報
第2の暗号化キー（Kw）
契約情報
第3の暗号化キー
制御信号
SW
送信側
受信側

【図９】


第2の期間
T1
T2
T3
第1の暗号化キー（Ks）
送信される
第2の暗号化キー（Kw）
Kw2
Kw3
Kw4
送信されるECM情報の
解読に有効な
第2の暗号化キー（Kw）
Kw1
Kw2
Kw3
記憶手段7から出力される
第2の暗号化キー（Kw）
Kw1
Kw2
Kw3
記録再生手段8による
記録のタイミング
p1
p2
A
B